Questions juridiques à se poser lors de l'informatisation d'un service d'urgence

Deplanque, Laetitia; Verhaegen, Marie-Noelle

Published in:
Manuel d'informatisation des urgences hospitalières

Publication date:
2003

Document Version
le PDF de l'éditeur

MODULE « GARANTIE DE FONCTIONNEMENT CRYPTO-LEGAL »

CHAPITRE 2
ASPECTS JURIDIQUES

LAETITIA DEPLANQUE MARIE-NOËLLE VERHAEGEN

Prof. Dr YVES POULLET

Centre de recherches informatique & droit

Facultés universitaires Notre-Dame de la Paix, Namur

yves.poullet@fundp.ac.be

I. POUR QUELLE FINALITÉ L'INFORMATISATION DU SERVICE HOSPITALIER D'URGENCES EST-ELLE ENVISAGÉE ?

La détermination de la finalité précise d'un traitement de données personnelles relatives à des individus est fondamentale. C'est en effet cet objectif particulier de départ qui va orienter toutes les opérations liées au traitement.

Le présent exposé part du postulat suivant lequel l'informatisation du service d'urgences de l'hôpital se fait dans le cadre d'une *finalité thérapeutique*, de l'accomplissement des soins de santé.

Cette informatisation entendrait *participer à la qualité des soins de santé* en assurant une *meilleure circulation de l'information* relative au patient entre les différents intervenants aux soins[4].

II. QUELLES SONT LES SOURCES LÉGALES PRINCIPALES EN LA MATIÈRE ?[5]

a. **La loi du 8 décembre 1992 relative à la protection de la vie privée** à l'égard du traitement des données à caractère personnel (M.B., 18.03.1993) – appelée dans le présent exposé « loi vie privée » – vise à protéger l'individu face à l'utilisation des informations qui le concernent.

Le terme « traitement » utilisé dans la loi vie privée comprend toute opération ou ensemble d'opérations appliquées à des données personnelles. Il vise autant la collecte des données que leur

[4] Notons que si l'informatisation des données devait également servir (dans le même temps ou ultérieurement) pour des fins statistiques ou de recherches scientifiques, celle-ci devrait alors s'effectuer en conformité avec des règles particulières qui ne sont pas visées directement dans le présent exposé. Cf. notamment à cet égard le rapport de L. Deplanque et M.Verhaegen (CRID) : « La réutilisation des données à caractère personnel relatives à la santé en recherche médicale, sous l'angle de textes internationaux et plus particulièrement sous l'angle du droit belge », à publier.

[5] Les textes législatifs auxquels le présent exposé fait référence peuvent être trouvés sur le site : http://www.just.fgov.be - Voir rubrique « sources du droit » et sous rubrique « législation consolidée ».

conservation, leur utilisation, leur modification, leur communication, etc.

La loi vie privée modifiée en 1998 et entrée en vigueur le 1er septembre 2001 instaure un devoir de *loyauté et de transparence* l'égard de la personne concernée quant à l'existence du traitement des données, à l'objectif de celui-ci et à la manière dont il fonctionne.

La loi octroie également à la personne concernée des *droits qu'elle pourra elle-même mettre en œuvre* et que l'on résume par la notion de droit à l'autodétermination.

Dans la mesure où les données *relatives à la santé* sont particulièrement sensibles ou susceptibles de créer des discriminations dans l'octroi de certains droits, la loi vie privée part du principe suivant lequel *le traitement de ces données est* a priori *interdit sauf dans le cadre de certaines hypothèses.* Et parmi ces hypothèses, l'on retrouve la possibilité de traitement de données relatives à la santé à des fins thérapeutiques. La loi *autorise* en effet le traitement des données relatives à la santé « lorsque le traitement est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé » (article 7, §2, j de la loi).

Dans le contexte des soins, le respect des dispositions de la loi vie privée s'inscrit dans la nécessité de maintenir la confiance du patient envers le secteur des soins de santé.

b. Lors de l'informatisation des données relatives à la santé, les praticiens professionnels devront tenir compte de leur **obligation légale au secret professionnel** (en l'occurrence le secret médical) telle que prévue dans l'article 458 du Code pénal. Cette obligation se justifie par *l'exigence de confiance* qui doit régner *entre le patient et le praticien* qui le soigne. Le secret médical vise non seulement à protéger les intérêts individuels du patient mais également l'intérêt de la société en permettant à chaque citoyen de bénéficier de soins avec la garantie que ce qu'il sera amené à confier restera sous le sceau de la confidence.

L'obligation au secret concerne les praticiens professionnels intervenant dans une relation de soins (médecins, infirmières, kinésithérapeutes, etc.) mais aussi tous leurs collaborateurs obligés, en l'occurrence les secrétaires, téléphonistes, stagiaires,

ambulanciers du service 100, sans excepter le personnel du service d'accueil hospitalier.

En sus de la loi pénale, le Code de déontologie médicale donne en ses articles 56 et suivants une description précise et complète du secret professionnel médical. Le *champ d'application* du secret médical est large puisque, selon ce code, le confident nécessaire ne peut révéler à quiconque ce qu'il a constaté, vu, connu, appris, découvert ou surpris dans l'exercice ou à l'occasion de l'exercice de sa profession.

L'interdiction de divulguer des données à des tiers ne peut être *levée* que dans des hypothèses strictement déterminées, à savoir, au regard de l'article 458 du Code pénal, lorsque *la loi* contraint le dépositaire à révéler le secret ou en cas de *témoignage en justice.*

L'article 58 du Code de déontologie médicale reprend les différentes exceptions légales à l'obligation au secret du médecin, sachant que le législateur a finalement non seulement prévu des cas d'« obligation » de divulgation de données par celui-ci à des tiers mais aussi des cas de «possibilité» de communication. Le code de déontologie énumère ainsi :

- La communication, dans le cadre de la législation sur l'assurance maladie invalidité, aux médecins inspecteurs du service du contrôle de l'INAMI des seuls renseignements nécessaires à l'exercice de leur mission de contrôle dans les limites strictes de celles-ci. La communication de ces renseignements et leur utilisation par les médecins inspecteurs sont subordonnées au respect du secret professionnel ;
- La communication aux médecins-conseils des organismes assureurs en matière de l'Assurance Maladie Invalidité et dans les limites de la consultation médico-sociale de données ou des renseignements médicaux relatifs à l'assuré. Le médecin-conseil d'un organisme assureur est, comme tout médecin, tenu de respecter le secret professionnel ; il ne doit donner à cet organisme que ses seules conclusions sur le plan administratif ;
- La déclaration aux inspecteurs d'hygiène des maladies transmissibles épidémiques, suivant les modalités et conditions prévues par la législation en la matière ;
- L'envoi à l'inspecteur d'hygiène de rapports concernant les maladies vénériennes en application de la législation relative à la prophylaxie de ces maladies ;

- Les communications et les déclarations à l'officier de l'état civil en matière de naissance conformément aux dispositions légales ;
- La délivrance de certificats médicaux réglementaires en vue de permettre les déclarations d'accidents de travail et contenant toutes les indications en rapport direct avec le traumatisme causal ;
- La délivrance de rapports et certificats médicaux en exécution des prescriptions légales relatives à la protection de la personne des malades mentaux et à la protection des biens des personnes totalement ou partiellement incapables d'en assumer la gestion en raison de leur état physique ou mental ;
- La délivrance de rapports médicaux en exécution des prescriptions légales relatives aux maladies professionnelles ;
- La délivrance de certificats médicaux en exécution des prescriptions légales relatives aux contrats d'assurance terrestre.

L'on peut encore citer, parmi les exceptions à la règle du secret du soignant, les dispositions légales particulières relatives à la maltraitance des enfants (art. 458 bis du Code pénal) ainsi que les situations exceptionnelles d'état de nécessité, là où un péril grave et imminent est en cause.

Une dernière permission de dérogation à la règle du secret et qui devra particulièrement retenir l'attention lors de l'informatisation du service hospitalier est la situation du *secret médical partagé.*

La théorie du secret médical partagé permet la communication d'informations entre les praticiens soignant un même patient et ce, moyennant le respect de plusieurs conditions :

- la communication de renseignements par un praticien professionnel ne peut se faire que dans l'intérêt du patient, à l'égard d'un autre praticien tenu au secret et chargé de poursuivre l'élaboration du diagnostic ou des soins du patient ;
- la communication doit être limitée aux données utiles et nécessaires à la mission (du moment) du destinataire des données ;
- la divulgation ne peut se faire que si le patient ne s'y oppose pas (ce qui implique que celui-ci en soit informé).

Sachant que, dans le cadre d'une *centralisation* de données médicales (que ce soit au sein de l'hôpital ou d'un service hospitalier

particulier), les destinataires des données ne sont pas nécessairement identifiés à l'avance par les praticiens professionnels qui auront encodé celles-ci, il s'agira d'implémenter les *garanties techniques* permettant d'assurer au mieux les conditions prévues ci-dessus (cf. infra, point V, a.5.).

c. La loi relative aux droits du patient du 22 août 2002 (*M.B.*, 26 sept. 2002), entrée en vigueur le 6 octobre 2002, concerne également le traitement informatisé des données du patient dans une finalité thérapeutique. Elle fixe notamment les *modalités d'accès du patient à son dossier médical* et précise les règles de la *communication* à la personne concernée (en l'occurrence le patient) des données relatives à sa santé qui font l'objet d'un traitement tel que visé par la loi vie privée. La loi sur les droits du patient prévoit également en son article 11 la création de la fonction d'un médiateur au sein de l'hôpital. Celui-ci est compétent pour gérer ou prévenir les plaintes relatives aux relations entre praticiens et patients.

Voyez aussi, à propos de cette loi sur les droits du patient, l'avis du Conseil national de l'Ordre des médecins du 26 juillet 2003 (cf. http ://www.ordomedic.be).

d. Deux arrêtés royaux pris en exécution de la loi sur les hôpitaux coordonnée le 7 août 1987 peuvent encore donner des indications quant au traitement des données visé dans le présent exposé. Il s'agit de *l'arrêté royal du 3 mai 1999 (M.B., 30.07.1999) relatif au dossier médical hospitalier* (voir les dispositions relatives au contenu du dossier, à sa durée de conservation et à son archivage) et de *l'arrêté royal du 23 octobre 1964 relatif aux normes auxquelles doivent répondre les hôpitaux et leurs services.* Ce dernier arrêté donne des précisions quant au règlement de l'hôpital pour le traitement des données du patient et quant à l'existence du conseiller en sécurité au sein de l'hôpital

III. QUI A UN POUVOIR DE DÉCISION QUANT À LA CONSTITUTION DU TRAITEMENT DES DONNÉES ?

Le responsable du traitement est celui qui fixe les finalités et les moyens du traitement. L'article premier, §4 de la loi vie privée le définit de la manière suivante : « Par responsable du traitement, on entend la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres,

détermine les finalités et les moyens du traitement de données à caractère personnel ».

Aucune disposition spécifique ne détermine qui, au sein de l'hôpital, doit être considéré comme le responsable du traitement des données du patient. À défaut de pareille disposition, il faut examiner qui, dans les faits, est susceptible de déterminer les moyens et finalités de ce traitement.

La loi du 7 août 1987 sur les hôpitaux confie au gestionnaire de l'hôpital la responsabilité générale et finale pour l'activité hospitalière, sur le plan de l'organisation et du fonctionnement, ainsi que sur le plan financier. Ce gestionnaire a également la charge de définir la politique générale de l'hôpital et de prendre les décisions de gestion.

L'on peut donc en déduire que sur le terrain, *le (directeur) gestionnaire de l'hôpital* aura un poids certain dans la détermination des moyens et finalités du traitement des données de l'hôpital et par conséquent du service d'urgences de celui-ci. Le gestionnaire de l'hôpital pourrait ainsi être judicieusement désigné comme responsable du traitement ou tout au moins avoir une voix prépondérante dans le choix de la personne qui assumera les missions dudit responsable.

Ceci étant, quelle que soit la personne désignée comme responsable du traitement, elle devra certainement *se concerter avec d'autres personnes ou organes de l'hôpital impliqués dans l'organisation de l'activité hospitalière* pour déterminer les finalités et moyens du traitement des données. L'on vise ainsi le directeur médical, chaque médecin-chef (en l'occurrence le médecin-chef du service d'urgences pour l'informatisation du service d'urgences), les infirmiers en chef, le conseil médical, le conseil infirmier et paramédical, le service informatique de l'hôpital, éventuellement le comité d'éthique hospitalier, etc.

IV. QUELS SONT LES ACTEURS PRINCIPAUX CONCERNÉS PAR L'INFORMATISATION DU SERVICE ?

a. Le responsable du traitement tel que défini ci-dessus est tenu d'assurer la majeure partie des obligations instaurées par ou en vertu de la loi vie privée (cf. infra, V.a.). Il peut, s'il le souhaite, confier ses tâches à un **sous-traitant**, lequel agira pour son compte (cf. infra).

Sachant que le responsable du traitement ne sera pas nécessairement un praticien soignant le patient, il devra éviter d'accéder directement au contenu des données du patient, eu égard à la règle du secret médical. S'il ne peut faire autrement que de connaître certaines données dans le cadre de l'exécution de ses missions, il sera tenu à la règle de confidentialité telle que rappelée à l'article 25, 3° de l'A.R. du 13 février 2001 pris en vertu de la loi vie privée.

b. S'agissant spécifiquement du traitement des données *relatives à la santé,* l'article 7, §4 al.1 de la loi vie privée impose que le traitement se fasse **sous la responsabilité d'un professionnel de la santé.** Ce dernier pourrait être – mais pas obligatoirement – le responsable du traitement tel que visé ci-dessus.

L'article 7, §2, j de la loi vie privée précise en outre que dans le cadre d'un traitement de données relatives à la santé *à finalité thérapeutique*, le traitement doit se faire sous **la surveillance d'un professionnel des soins de santé.** L'on peut raisonnablement considérer que le professionnel de la santé « responsable » des données de santé (point b) est la même personne que le professionnel de la santé « surveillant », visé ici. Ses missions seront envisagées plus loin.

La notion de « professionnel des soins de santé», responsable et surveillant des données relatives à la santé, n'est pas définie dans la loi vie privée. L'on peut toutefois considérer qu'elle se rapproche de la notion de « praticien professionnel » visée dans la loi sur les droits du patient, à savoir le professionnel ayant un *diplôme relatif à la prestation de soins.* Dans le cadre d'un réseau impliquant la centralisation de données médicales encodées (que ce soit pour tout l'hôpital ou le service d'urgences en particulier), ce professionnel qui chapeaute l'organisation de la circulation des données relatives à la santé ne prestera toutefois pas nécessairement des soins au sein de l'hôpital. Le médecin spécialisé en gestion des données de santé, tel que prévu dans l'A.M. du 15 octobre 2001, pourrait par exemple être une personne exerçant ces missions de responsabilité et surveillance des données relatives à la santé (cf. infra).

c. Le conseiller en sécurité

Selon l'A.R. du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux doivent répondre, le responsable du traitement doit désigner un conseiller en sécurité chargé d'assurer la

sécurité et la confidentialité de l'information circulant au sein de l'hôpital.

d. Les praticiens professionnels, utilisateurs du traitement

Les praticiens soignant les patients en service d'urgences sont les premiers concernés par l'informatisation de ce service. Ce sont eux qui vont utiliser le système afin d'accomplir leurs missions thérapeutiques.

Conformément à l'A.R. n°78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé, les conditions liées au *diplôme* donnant droit au titre de praticien professionnel de la santé ou à la qualification de professionnel stagiaire devront être réunies pour encoder les données traitées par le service d'urgence ou pour accéder à ces dernières.

Pour le surplus, il faut s'assurer que le praticien ne traite des données d'un patient que s'il *a lui-même en charge le patient dans le cadre des soins à prodiguer à ce dernier.*

Dans ce contexte, un médecin-conseil d'une société d'assurance, par exemple, ne pourrait évidemment jamais avoir accès au système informatique du service d'urgences.

La question du rôle des *collaborateurs obligés (non soignants)* des praticiens *(par exemple, secrétaires, service d'accueil hospitalier, etc.)* sera envisagée dans la partie relative à la détermination des destinataires des données (V, a.2.) et à l'encodage des données par lesdits praticiens (V, e.3.).

e. Les patients

Les patients sont bien entendu concernés par l'informatisation du service d'urgences car ce sont les données relatives à leur propre santé qui feront l'objet de l'informatisation.

Le patient est loin de devoir rester passif ; il peut avoir un rôle important à jouer, d'une part par la revendication de certains droits (cf. infra) et d'autre part par l'octroi d'informations de qualité qu'il confiera lui-même au praticien et desquelles dépend l'utilité même du système informatique.

f. L'hôpital

L'informatisation d'un service hospitalier met en cause le fonctionnement de l'hôpital lui-même. Elle doit être compatible avec les systèmes informatiques des autres services et éventuellement

être raccordée au dossier informatique hospitalier centralisé (unique) s'il en existe un.

Le responsable du traitement du service hospitalier (d'urgences) est d'ailleurs le responsable du traitement de tout l'hôpital.

Nous l'avons dit, dans le cadre de ses missions et obligations (et particulièrement au niveau de l'instauration des mesures techniques et organisationnelles à des fins de sécurité), le responsable du traitement devra parfois se concerter avec *d'autres personnes ou organes de l'hôpital impliqués dans l'organisation* de celui-ci. Le *service informatique* de l'hôpital sera notamment amené à travailler avec le responsable du traitement, au regard des finalités et moyens que celui-ci aura fixés et sous son autorité.

Par ailleurs, les conflits éventuels à propos des droits du patient en matière de télématique médicale (ex : au niveau de l'accès au dossier informatisé) pourront faire l'objet d'une intervention du *médiateur hospitalier* prévu dans la loi sur les droits du patient (cf. supra, II, c).

V. QUELS SONT LES DROITS ET OBLIGATIONS DES ACTEURS CONCERNÉS ?

a. Le rôle du responsable du traitement

a.1. Vérification des conditions préalables de légitimité et licéité du traitement des données (article 4, §1, 1° et 2 ° de la loi vie privée)

La loi vie privée interdit, comme nous l'avons déjà dit, le traitement des données relatives à la santé sauf exceptions. Et parmi ces exceptions, l'article 7, §2, j légitime le traitement informatisé des données relatives à la santé *dans un but thérapeutique.*

Ceci dit, même si le traitement informatisé du service d'urgence est ainsi « a priori » légitime, le responsable de celui-ci devra encore vérifier si le traitement des données envisagé répond à la condition de la *proportionnalité* : il devra s'assurer qu'il n'y a pas une disproportion entre, d'une part, l'intérêt et les avantages apportés par le traitement informatisé et, d'autre part, les atteintes (ou risques

d'atteintes) aux droits fondamentaux des patients dont on traitera les données.

Le principe de légitimité implique également que les données ne peuvent être traitées ultérieurement de manière incompatible avec les objectifs annoncés au patient.

Le responsable du traitement devra veiller à ce que la mise en place du traitement informatisé des données soit *licite*, c'est-à-dire qu'elle soit respectueuse de toutes les dispositions légales et réglementaires qui la concerne.

Par conséquent, le traitement des données à des fins thérapeutiques devra non seulement être en concordance avec la loi vie privée mais également permettre aux intervenants à l'informatisation de respecter toutes leurs obligations légales, telles les obligations relatives au secret médical, à la tenue du dossier du patient, etc.

a.2. Détermination des types de données à traiter et détermination des catégories de destinataires des données

L'A.R. du 13 février 2001 pris en vertu de la loi vie privée impose que le responsable du traitement désigne les *catégories de personnes* ayant accès aux données à caractère personnel relatives à la santé avec une *description précise de leur fonction par rapport au traitement* des données visées. Cette liste doit être tenue à la disposition de la Commission de protection de la vie privée.

La loi vie privée (article 16, §2, 2°) précise encore que, pour les personnes agissant sous l'autorité du responsable du traitement, l'accès aux données ainsi que les possibilités de traitement sont *limités* à ce dont ces personnes *ont besoin* pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service.

Dans le cadre d'une centralisation de données des patients, le responsable du traitement devra donc déterminer à l'avance qui est susceptible de traiter les données relatives au patient et à quel type de données chaque utilisateur aura accès en fonction de ses spécialités et compétences.

Ce principe correspond également à la théorie du secret partagé, suivant laquelle *seules les données (du patient) utiles et nécessaires à la mission d'un praticien peuvent être communiquées à ce dernier.*

En pratique, la gestion de l'accès aux données *relatives à la santé* en fonction de la spécialité et de l'identité du praticien soignant n'est pas nécessairement évidente, surtout dans un service d'« urgences » où

l'on pourrait considérer que chaque praticien soignant devrait avoir accès à toutes les données de santé relatives au patient. Ceci dit, le débat doit se poser au sein de l'hôpital et du service. Le responsable du traitement devra être clair en la matière. Il devra répondre à la question suivante : à quelles données auront accès les médecins du service de telle spécialité, les stagiaires de ceux-ci, les infirmières, etc. ?

Ce qui devrait à tout le moins apparaître dans le cadre de l'informatisation des données du patient, c'est une séparation de celles-ci en fonction de leur « nature » (cf. ci-dessous). Ainsi, toutes les données médicales ne seraient pas nécessairement accessibles à tous les collaborateurs « non soignants » des praticiens (par exemple, secrétaires, service comptable, service social, service d'accueil, etc.).

À cet égard, le *Conseil de l'Europe* (Rec. N°R(97) 5 du 13 février 1997 du Comité des ministres aux États membres relative à la protection des données médicales), relayé par le Conseil national de l'Ordre des médecins, recommande en vue d'une part, de *l'accès sélectif* aux données et, d'autre part, de la sécurité des données médicales, que leur traitement soit en règle générale conçu de façon à permettre la *séparation :*

- *des identifiants et des données relatives à l'identité des personnes ;*
- *des données administratives ;*
- *des données médicales ;*
- *des données sociales ;*
- *des données génétiques.*

Par ailleurs, le responsable du traitement devra également savoir que selon la loi sur les droits du patient, le patient pourra avoir directement accès à toutes les données de santé le concernant, exceptées les *données relatives aux tiers* et les *annotations personnelles* des praticiens. Quant aux données *estimées comme relevant du privilège thérapeutique* (données sensibles que le praticien estime ne pouvoir être consultées par le patient que de manière indirecte), elles ne pourront être consultées que par l'intermédiaire d'un praticien professionnel désigné par ce dernier. Dans le cadre de l'informatisation des données, il serait donc sans doute judicieux de *cibler toutes ces données,* de manière à ce que le

patient n'y ait pas accès lors de la demande de consultation de son dossier.

a.3. Fixation de la procédure d'information au patient

- En application de l'article 9 de la loi vie privée, le responsable du traitement *est tenu de veiller à ce que le patient soit informé* de l'existence et des diverses modalités du traitement des données qui le concernent.

Cette obligation est fondamentale. Elle constitue la pierre angulaire de la loi vie privée en traduisant les principes de transparence et de loyauté qu'elle entend mettre en œuvre. Le responsable du traitement peut confier cette tâche d'information à la personne en contact avec le patient ou amenée à récolter les données auprès de celui-ci.

- Si la loi vie privée mentionne déjà les informations à communiquer au patient (article 9 et article 25 à 27 de l'A.R. du 13 mars 2001 pris en vertu de cette loi), l'A.R. du 23 octobre 1964 « portant fixation des normes auxquelles les hôpitaux doivent répondre » précise davantage les *différents éléments* à porter à la connaissance du patient :

- les finalités du traitement des données à caractère personnel ;
- l'identité et les coordonnées du responsable du traitement et de la personne qui peut agir en son nom ;
- la base légale ou réglementaire qui autorise le traitement des données (cela permet de contrôler sur quoi il se base pour traiter des données en principe interdites...) ;
- le nom du médecin qui exerce la responsabilité et la surveillance du traitement des données (désigné par le responsable du traitement) ;
- le nom du conseiller en sécurité chargé de la sécurité de l'information ;
- les catégories de personnes dont les données font l'objet d'un traitement ;
- la nature des données traitées et la manière dont elles sont obtenues ;
- l'organisation du circuit des données médicales à traiter ;
- la procédure suivant laquelle, si nécessaire, les données sont rendues anonymes ;

- les procédures de sauvegarde afin d'empêcher la destruction accidentelle ou illicite de données, la perte accidentelle de données ou l'accès illicite à celles-ci, leur modification ou diffusion illicite ;
- le délai au-delà duquel les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;
- les rapprochements, interconnexions ou toute forme de mise en relation de données faisant l'objet du traitement ;
- les interconnexions et les consultations ;
- les cas où les données sont effacées ;
- la manière dont les patients peuvent exercer leurs droits visés dans la loi vie privée du 8 décembre 1992.

- L'A.R. du 23 octobre 1964 précise qu'au sein d'un hôpital, l'information au patient s'effectue en principe par *la remise d'office d'un exemplaire du règlement relatif à la protection de la vie privée.*

Il appartiendra au responsable du traitement d'imaginer la manière la plus efficace et la plus pédagogique d'informer les patients au regard de ces principes.

Par ailleurs, les informations dues au patient doivent lui être fournies *au plus tard au moment où les données sont récoltées auprès de lui, ou, si celles-ci ont été récoltées auprès de tierces personnes, au moment de leur enregistrement ou de leur première communication à un tiers.*

- Dans un contexte d'urgence, les règles visées ci-dessus peuvent être nuancées. Face à un patient inconscient ou lorsque son état nécessite une intervention urgente, l'information devrait pouvoir être postposée jusqu'à ce que le patient soit en état de la recevoir.

Entre-temps, l'information sur le traitement des données devrait-elle ou pourrait-elle être communiquée au « représentant » du patient tel que prévu dans la loi relative aux droits du patient ? Si la réponse est claire en ce qui concerne les représentants des enfants présentés en urgence, elle l'est moins pour les mineurs adolescents ou les adultes incapables de fait. Nous pouvons toutefois affirmer que cette solution est envisageable, dans la mesure où la loi sur les droits du patient confère de larges droits au représentant de ces patients telle, dans une certaine mesure, la consultation de leur dossier (articles 12 à 15). Il n'est dès lors pas inadéquat d'informer ces représentants du patient sur le « traitement » informatisé des données le concernant.

- Revenant au principe du devoir d'information à l'égard du patient, l'on rappellera qu'en application de la théorie du secret médical partagé, le patient doit être informé des « communications » de données d'un professionnel à un autre, pour pouvoir éventuellement s'y opposer.

C'est ainsi que le responsable du traitement devra, dans le cadre de l'information « préalable » à accorder au patient, indiquer les modalités de fonctionnement du réseau impliquant des « transferts potentiels » de données entre professionnels. Le responsable devrait pouvoir répondre à la question suivante : qui, *a priori*, est susceptible de recevoir une information relative au patient et à quel type de données aura-t-il normalement accès ? L'on revient ainsi à l'obligation, pour le responsable du traitement, de déterminer les types de données à traiter et les catégories de destinataires des données (*point a.2.*)

Pour le surplus, il reviendra aux professionnels utilisateurs du traitement d'informer, dans la mesure du possible et au coup par coup, des opérations qu'ils effectuent dans le cadre du réseau, ce dernier étant accessible aux différents professionnels du service.

a.4. Mesures d'information à l'égard des utilisateurs à propos de la collecte de données (auprès du patient), de leur pertinence, de leur exactitude et de leur limitation de conservation dans le temps

Les articles 4, §1, 3°,4°,5° et 7 §5 de la loi vie privée apportent des indications quant à la collecte et autres opérations de traitement des données différentes : les données – si elles sont relatives à la santé – doivent être collectées auprès de la personne concernée (sauf exceptions, cf. infra) ; les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ; les données doivent être exactes et, si nécessaire, mises à jour ; les données doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues.

Il appartiendra au responsable du traitement d'avertir et d'informer les utilisateurs du traitement sur ces mesures, de manière à ce que ces derniers, seuls susceptibles de traiter et accéder aux données en raison de la règle du secret professionnel, puissent les appliquer correctement (cf. infra).

a.5. Fixation de la politique à mener en matière de confidentialité et de sécurité

Le responsable du traitement doit prendre toutes les mesures nécessaires afin de garantir la confidentialité et la sécurité des données à caractère personnel.

Celles-ci seront assurées par des obligations de secret et de confidentialité, d'une part, et par l'adoption des mesures techniques et organisationnelles, d'autre part.

a) Les obligations au secret et à la confidentialité

- La règle du secret professionnel, applicable à *tous les praticiens soignant* les patients et à leurs *collaborateurs obligés*, participe à la sécurité du traitement (art.458 C. pénal).

- *Le professionnel des soins de santé sous la responsabilité duquel* est effectué le traitement de données à caractère personnel relatives à la santé (cf. supra) est soumis au secret lors du traitement, de même que ses préposés ou mandataires (art 7, §4, al.3 de la loi vie privée).

- Lors du traitement, le responsable du traitement doit veiller à ce que *toutes les personnes qui ont accès aux données relatives à la santé* soient tenues au respect du caractère confidentiel des données traitées, par une obligation légale, statutaire ou par une disposition contractuelle équivalente. (art. 25, 3° de l'A.R. du 13 février 2001 pris en vertu de la loi vie privée). Cette mesure s'avère particulièrement importante pour les utilisateurs des données de santé qui ne sont pas les confidents nécessaires du patient (praticiens) ni leurs collaborateurs obligés « directs » (secrétaires), tels par exemple les informaticiens de l'hôpital, etc.

b) Les mesures techniques et organisationnelles

La protection de la vie privée et le respect du secret médical imposent l'adoption de mesures techniques et organisationnelles destinées à assurer la sécurité du traitement des données du patient.

- En sus des dispositions de l'article 16 de la ***loi vie privée*** relatives au choix du sous-traitant, à la diligence à manifester en ce qui concerne la qualité des données traitées, à la détermination des responsabilités des personnes agissant sous son autorité et à l'information à octroyer à ces dernières, l'article 16, §4 de la loi vie privée prévoit que « le responsable du traitement doit prendre toutes les mesures techniques et organisationnelles nécessaires afin de protéger les données contre la destruction accidentelle ou non

autorisée, contre la perte accidentelle, ainsi que contre la modification, l'accès et tout autre traitement non autorisé des données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat ».

Ce niveau sera apprécié au regard, d'une part, de l'état de la technique et des frais qu'entraîne l'application de ces mesures, et d'autre part, de la nature des données à protéger des risques potentiels. Les données médicales étant des données sensibles, le niveau de protection devra être plus élevé que pour d'autres données.

Par ailleurs, comme nous l'avons déjà précisé, l'accès aux données et les possibilités de traitement par les utilisateurs de celui-ci doit être limité en fonction de leurs missions et leurs besoins.

La liste contenant les catégories de personnes ayant accès aux données relatives à la santé devra être mise à la disposition de la Commission pour la protection de la vie privée et portée à la connaissance des patients eu égard à la théorie du secret médical partagé.

- Le ***Conseil de l'Europe*** préconise la prise de mesures appropriées pour assurer la confidentialité, l'intégrité et l'exactitude des données traitées (Rec. N°R(97) 5 du 13 février 1997 du Comité des Ministres aux États membres relative à la protection des données médicales, art. 9.2), ces mesures devant viser :

- à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations) ;
- à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données) ;
- à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire) ;
- à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation) ;

- en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation : des identifiants et des données relatives à l'identité des personnes ; des données administratives ; des données médicales ; des données sociales ; des données génétiques (contrôle d'accès) ;
- à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication) ;
- à garantir qu'il puisse être vérifié et constaté *a posteriori* qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction) ;
- à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport) ;
- à sauvegarder les données par la constitution de copies de sécurité (contrôle de disponibilité).

- Le Conseil national de l'Ordre des Médecins a, quant à lui, rendu divers avis en matière de sécurité de traitement de données à caractère personnel relatives à la santé dans un contexte thérapeutique (cf. www.ordomedic.be).

Voyez ainsi les avis suivants : « Communications électroniques-secret médical », 22 avril 1995 ; « Télématique médicale »,15 février 1997 ; « Dossier médical global informatisé », 12 décembre 1998 ; « Sécurité des données transmises par internet », 20 février 1999 ; « Dossier médical et infirmier électronique », 17 février 1999 ; avis du 17 février 2001 relatif à la protection de la confidentialité lors de la transmission de données médicales à caractère personnel par le réseau internet (chiffrement et signature électronique) ; avis du 15 juin 2002 relatif à la tenue de bases de données médicales contenant des données nominatives ou identifiables.

- Concrètement, plusieurs aspects retiennent l'attention.

1. Il s'agit de déterminer les utilisateurs potentiels du système et de poser les règles de leur identification au niveau de l'accès au système informatique, par exemple par le biais de l'insertion

d'une carte professionnelle, d'un mot de passe, d'une empreinte digitale, etc.

Il s'agit de prévoir un moyen d'identification qui soit strictement personnel à chaque utilisateur et qui indique sa fonction (spécialisation, etc.) au sein de l'hôpital.

2. Il s'agit de séparer les identifiants et données relatives à l'identité des personnes, des données administratives, des données médicales, des données sociales, des données génétiques (contrôle d'accès) en précisant qui est susceptible d'accéder à chaque catégorie d'entre elles.
3. Il s'agit de savoir si certaines personnes, tout en étant autorisées à encoder des données « pour le compte » d'une autre personne (cf. infra, collaborateurs directs, par exemple, les secrétaires) doivent pour autant avoir accès aux données auxquelles le praticien mandant peut lui-même avoir accès (volet « encodage » séparé du volet « consultation » pour ces personnes collaboratrices ?).
4. Il s'agit de limiter dans le temps la possibilité d'accès au système (en fonction des missions des utilisateurs et des données concernées).
5. Il s'agit de déterminer les garanties permettant de s'assurer que le praticien qui traite les données relatives à la santé a bien en charge le patient ou, tout au moins, qu'il fait partie du service où est censé être le patient (il s'agit d'éviter que n'importe quel médecin de l'hôpital – n'ayant pas en charge le patient – ait accès au dossier).
6. Il s'agit de déterminer les données auxquelles le praticien soignant le patient peut avoir accès. En principe, il ne peut avoir accès qu'aux données nécessaires à l'exercice de son art. En pratique, cette détermination est loin d'être aisée. Le débat doit avoir lieu au sein du service hospitalier concerné et de l'hôpital en général.
7. Les mesures telles que l'installation d'un détecteur de virus, d'un système de sauvegarde automatique, du dédoublement des bases de données, la conservation du traitement dans un lieu sûr, le respect des normes de chiffrement précisées par le Conseil national de l'Ordre des médecins en cas d'utilisation de l'internet, etc. ne sont pas à négliger .

8. La question de la disponibilité des données, de leur intégrité et de leur imputabilité au praticien est essentielle (cf. aussi infra, utilisation de la signature électronique pour l'encodage de certains documents).
9. Un **système de traçabilité** des accès et des opérations effectuées sur les données du patient devra être mis en œuvre afin de permettre le contrôle *a posteriori* des utilisateurs et des utilisations des données.

a.6. Déclaration à la Commission de la protection de la vie privée

Avant de mettre en œuvre un traitement entièrement ou partiellement automatisé, le responsable du traitement doit déclarer le traitement auprès de la Commission de la protection de la vie privée (article 17).

Le formulaire de déclaration peut être directement accessible sur le site Internet (http :/www.privacy.fgov.be) de la Commission. Une contribution est à verser pour chaque déclaration : 25 euros (1008 francs belges) si la déclaration est présentée sur support magnétique ou 125 euros (5042 francs belges) si la déclaration est présentée sur papier.

La déclaration doit contenir plusieurs éléments :

- la date de la déclaration et, le cas échéant (d'office pour les données relatives à la santé), la mention de la loi, du décret, de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé ;
- les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et le cas échéant, de son représentant en Belgique ;
- la dénomination du traitement automatisé ;
- la finalité ou l'ensemble des finalités liées du traitement automatisé ;
- les catégories de données à caractère personnel qui sont traitées (celles-ci étant en l'occurrence des données relatives à la santé, il en faut une description précise)
- les catégories de destinataires à qui les données peuvent être fournies ;

- les garanties dont doit être entourée la communication de données aux tiers ;
- les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit ;
- la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;
- une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement.

La Commission pourra demander les informations supplémentaires qu'elle juge pertinentes.

b. Le rôle du sous-traitant du responsable du traitement

Le responsable du traitement peut confier ses tâches à un sous-traitant. L'article premier, §5 de la loi vie privée défini le sous-traitant comme : « *La personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données.* »

Le responsable du traitement doit être prudent dans son choix du sous-traitant. Il doit s'assurer que celui-ci répond à plusieurs conditions de qualité.

Le responsable du traitement doit (article 16) :

- choisir un sous-traitant qui apporte les garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements ;
- veiller au respect de ces mesures, notamment par la stipulation de mentions contractuelles ;
- fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement ;
- convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu ;

consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences de traitement sur instruction du responsable.

c. Le rôle du surveillant et responsable des données relatives à la santé

Le rôle du surveillant et responsable des données relatives à la santé tel que décrit ci-dessus n'a malheureusement pas été défini dans la loi.

L'on peut considérer que celui-ci, n'étant pas nécessairement le responsable du traitement, assiste et conseille ce dernier dans ses tâches, eu égard à son expérience et ses connaissances quant aux caractéristiques des données de santé, à leur utilité et à leur pertinence au sein du réseau.

N'étant pas nécessairement un médecin soignant les patients dont les données sont traitées, il devra naturellement éviter d'accéder au contenu desdites données, eu égard à la règle du secret médical. S'il ne pouvait toutefois faire autrement que de connaître ces données dans le cadre de sa propre mission, il devra respecter son obligation à la confidentialité, telle que reprise à l'article 7, §4 de la loi vie privée.

d. Le rôle du conseiller en sécurité

Le conseiller en sécurité chargé de la sécurité de l'information au sein de l'hôpital et désigné par le responsable du traitement « doit veiller à la sécurité des applications et à la prise de mesures techniques et organisationnelles appropriées de manière à garantir le respect de la confidentialité des données ; il doit également veiller au contrôle des accès et autres » (Avis n°33/2002 du 22 août 2002 de la CPVP).

Le conseiller en sécurité interne devrait présenter des garanties d'indépendance face aux intérêts de l'institution hospitalière pour laquelle il travaillera.

S'il ne pouvait éviter d'accéder au contenu de données relatives à des patients identifiés, dans le cadre de son travail, il devra respecter son obligation à la confidentialité telle que prévue à l'article 25, 3° de l'A.R. du 13 février 2001 pris en vertu de la loi vie privée.

e. Le rôle des praticiens professionnels, utilisateurs du traitement

e.1. Respect des conditions d'accès

Chaque praticien veillera à n'accéder au système informatique que s'il a en charge le patient, si cela est utile et nécessaire pour sa mission et moyennant son propre code d'accès.

L'on sait que dans certains services hospitaliers, il arrive que l'ordinateur reste connecté pendant un certain temps après l'insertion du code d'accès d'un utilisateur. Des données peuvent alors être traitées (consultées ou encodées) par un autre utilisateur que celui qui a inséré son code d'accès.

Il s'agit d'éviter ce genre de scénario dans la mesure du possible et suivant les circonstances du moment, et ce, même si dans un service tel que celui des urgences, les données sont probablement toutes accessibles de la même manière aux différents médecins et stagiaires dudit service.

L'on recommandera donc la prudence et la vigilance en la matière. L'utilisateur qui a inséré son code d'accès pourrait être considéré comme responsable de la (non) qualité de toutes les données encodées par d'autres (sans qu'il en ait donné l'instruction) en suite de l'insertion de son propre code d'accès. Cet utilisateur pourrait éventuellement être – pour partie – tenu pour responsable des « fuites » quant à la consultation du système par des personnes non autorisées en suite de l'insertion de son propre code...

e.2. Respect des conditions liées à la collecte des données, à la pertinence des données traitées, à leur exactitude, à leur conservation limitée dans le temps

- L'article 7, §5 de la loi vie privée prévoit que les données à caractère personnel relatives à la santé doivent être **collectées auprès de la personne concernée.**

De manière subsidiaire et donc à titre exceptionnel, la loi vie privée prévoit que ces données relatives à la santé peuvent toutefois être collectées auprès d'une autre source à condition que ce soit nécessaire aux fins du traitement de données ou que la personne concernée (ici le patient) ne soit pas en mesure de les fournir.

Pour le cas où, en situation d'urgence, des données devaient être *collectées auprès d'un tiers* (par exemple, d'un proche du patient) *ou auprès d'un médecin* ayant soigné préalablement le patient, il est à tout le moins *essentiel que la personne concernée en soit avertie.* Elle devra être avertie (si elle est en état) au moment de l'enregistrement des données ou au moment de leur première communication à un autre tiers.

Eu égard à la théorie du secret partagé et dans le cadre d'une centralisation de données accessibles à différents praticiens, l'on a déjà vu que le patient devra avoir été *informé* des modalités de fonctionnement du système impliquant des *transferts* possible de données entre thérapeutes. Par ailleurs, si c'est possible et praticable, le professionnel traitant les données devrait informer au coup par coup le patient des opérations qu'il effectue dans ce cadre.

- Le patient a droit à ce que ses données soient « **adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement » (art.4, §1, 3° loi vie privée).

Dans une relation thérapeutique, l'adéquation, la pertinence et le caractère non excessif des données traitées s'apprécient d'abord au regard de la finalité des soins.

- Le caractère d'**exactitude** que les données doivent présenter signifie que l'information doit être conforme à la réalité, complète et mise à jour si nécessaire. Il s'apprécie en fonction de la finalité poursuivie.

Il appartient au responsable du traitement de prendre les mesures nécessaires pour que les praticiens professionnels en charge du patient, seuls susceptibles de traiter directement les données en raison de la règle du secret médical, mettent eux-mêmes à jour les données ou rectifient celles qui sont inexactes ou incomplètes.

Dans le cadre de la médecine, il n'est pas toujours aisé de considérer si les données sont « exactes » ou non, certaines d'entre elles relevant d'appréciations subjectives, demeurant hypothétiques ou non définitives... Le diagnostic d'un médecin peut différer de celui d'un autre, ce qui témoigne de la marge d'appréciation thérapeutique.

Par ailleurs, si l'on peut concevoir qu'un praticien rectifie une donnée qu'il a lui-même encodée – la trace de la première donnée encodée devant toutefois rester – , il est difficile d'imaginer que, dans le cadre d'un dossier médical « partagé », alimenté et utilisé par plusieurs

praticiens d'un même service, l'un d'eux efface ou corrige purement et simplement une donnée encodée par un collègue.

Une procédure devrait être établie pour résoudre une éventuelle contestation entre plusieurs praticiens à propos d'une même donnée. À cet égard, les praticiens concernés (et éventuellement le patient) devraient pouvoir faire valoir leur point de vue. Ensuite, le résultat de la concertation devrait apparaître. En cas de correction d'une donnée antérieurement encodée, celle-ci devrait subsister en archivage et le fait de sa correction devrait apparaître et être mis en évidence à l'égard des différents utilisateurs du réseau.

- Les données ne doivent **être conservées que pour autant qu'elles soient nécessaires à la finalité poursuivie.** Les données doivent être *« conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement »* (art. 4, §1, 5° de loi vie privée).

Le but du traitement étant d'ordre thérapeutique, il appartiendra au responsable du traitement de veiller à ce que les médecins « référents » des patients (cf. infra, V, f.1.1.) soient attentifs au délai légal de conservation des données (actuellement de 30 ans, en vertu de l'article 46 du code de déontologie médicale et de l'article 1 §3 de l'A.R. du 3 mai 1999 sur le dossier médical hospitalier, eu égard à de possibles actions en responsabilité) à partir du moment où les patients sont arrivés au bout de leur traitement médical.

Après le délai légal de conservation du dossier, celui-ci sera archivé selon les modalités fixées par le responsable du traitement (en concertation avec le gestionnaire de l'hôpital si le responsable du traitement ne l'est pas lui-même) .

En tout état de cause, l'on pourrait considérer qu'après le traitement médical du patient ou le décès de celui-ci, le dossier « centralisé » et informatisé du patient ne devrait plus être accessible aux différents utilisateurs du traitement des données, si ce n'est au médecin « référent » du patient (cf. infra, V, f.1.1.).

e.3 Encodage en fonction de la compétence et la spécialisation concernée

L'encodage, qui constitue un traitement de données, devra respecter le prescrit de différentes règles.

De nombreux praticiens gravitent au sein ou autour du service d'urgences : le médecin urgentiste, l'anesthésiste, l'infirmier, le radiologue, les praticiens du laboratoire de biologie clinique, etc.

En principe, chaque praticien encodera les données résultant des actes qu'il a accomplis.

Plusieurs arrêtés royaux déterminent les actes qu'un praticien, en fonction de sa qualité et de sa spécialisation, peut poser. Le praticien encodera ainsi les données relevant des missions qu'il peut accomplir légalement.

À titre exemplatif, une infirmière ne pourrait en principe encoder des données relatives au diagnostic que le chirurgien a posé, l'élaboration d'un diagnostic chirurgical n'entrant pas dans son champ de compétences.

L'infirmière encodera les données relatives aux actes déterminés à l'article 21 quinquies de l'A.R. n°78 du 10 novembre 1967 et précisés dans l'A.R. du 18 juin 1990 « portant fixation de la liste des prestations techniques de soins infirmiers et de la liste des actes pouvant être confiés par un médecin à des praticiens de l'art infirmier, ainsi que des modalités d'exécution relatives à ces prestations et à ces actes et des conditions de qualification auxquelles les praticiens de l'art infirmier doivent répondre », *M.B.*, 26.07.1990 (modifié récemment dans un A.R. du 7 octobre 2002, M.B. 7.11.2002).

Autre exemple, si un pharmacien hospitalier devait encoder des données dans le traitement informatisé du service d'urgences, il devrait le faire en conformité avec l'article 4 de l'A.R. n°78 du 10 novembre 1967 précisant les tâches qui lui sont confiées ainsi qu'avec l'A.R. du 4 mars 1991 fixant les normes auxquelles une officine hospitalière doit satisfaire pour être agréée.

Cette exigence du respect des compétences est importante au regard de la responsabilité de chacun. En effet, chaque praticien est responsable des données qu'il encode. Dans un avis du 15 juin 2002, le Conseil national de l'Ordre des médecins signale que « l'enregistrement par le médecin de données personnelles médicales dans une base de données engage le responsabilité du médecin qui a la charge du patient... ».

- Ceci étant dit, l'encodage ne relevant pas directement de l'art de guérir lui-même, il n'est pas exclu que le praticien (notamment en situation d'urgence) *confie à un tiers la charge de l'encodage des données* relatives aux actes qu'il a lui-même posés.

Un avis du Conseil national de l'Ordre des médecins du 16 juillet 2002 mentionne notamment : « Le médecin en charge d'un dossier médical peut confier, sous sa responsabilité, certaines tâches administratives nécessitant pour les réaliser la connaissance d'une partie des éléments du dossier médical à des collaborateurs non-médecins. »

Dans cette hypothèse de délégation de tâches administratives (encodage), le praticien devra être attentif à suivre plusieurs *mesures de précaution.* En effet, le fait qu'un tiers procède à l'enregistrement des données n'enlève en rien la responsabilité du praticien quant aux données et à leur exactitude.

Ainsi, le praticien concerné devra avoir *lui-même* ouvert l'accès au réseau moyennant *son propre code*, de manière à ce que l'on sache qu'il est le responsable desdites données encodées par le tiers (à moins que le tiers n'ait un code d'accès spécial lui permettant d'encoder des données au nom d'un praticien identifié) ; le praticien devra prêter attention au *respect du secret médical dans le choix du tiers encodeur* (collaborateur obligé) et éviter de confier cette tâche à une personne non tenue au secret médical et extérieure à l'offre des soins : il devra *vérifier* a posteriori *l'exactitude* des données inscrites.

- Il est à remarquer que certains actes nécessitent la signature d'un médecin (cf. A.R. du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987 doit répondre, M.B. 30.07.1999). Dès lors, dans un projet d'informatisation des données, le recours à la signature électronique s'avérera nécessaire.

e.4. Respect du principe du secret médical partagé

Le praticien n'examinera que les données qui lui semblent nécessaires et utiles dans le cadre de sa mission.

Dans la mesure du possible, il dialoguera avec le patient à propos du traitement des données et l'informera des opérations qu'il effectue, surtout lorsqu'il est amené à encoder des données particulièrement sensibles et potentiellement accessibles par d'autres professionnels du service.

f. La place du patient

f.1. Que peut exiger le patient ?

f.1.1. Le droit à la consultation et à la communication des données

- L'article 9, § 2 de la loi relative aux droits des patients donne le droit au patient de consulter le dossier le concernant.

S'il le souhaite, le patient pourra se faire assister par une personne de confiance qu'il aura désignée et il peut aussi exercer ce droit par l'entremise de cette même personne.

Ce droit de consultation n'est pas absolu, *les annotations personnelles* du praticien ainsi que les *données concernant les tiers* en étant exclues.

La notion d'annotations personnelles a suscité de nombreux commentaires lors des travaux préparatoires de la loi. Dans ces derniers, il est fait référence aux notes que le praticien dissimule à des tiers, voire aux membres de l'équipe de soins. La non-consultation des annotations personnelles peut se justifier sur base de l'idée de l'intérêt supérieur que représente l'art de soigner par rapport à celui représenté par le droit d'accès. Le professionnel a un document de travail qui lui est réservé. Ce dernier ne pourrait, le cas échéant, être consulté que par l'intermédiaire d'un professionnel de la santé choisi par le patient.

Par ailleurs, une autre exception propre au droit médical vient limiter la portée de ce droit à la consultation : *l'exception thérapeutique* (art. 33 Code déontologie) consacrée par l'article 7, § 4 de la loi relative aux droits du patient. Dans l'hypothèse où le praticien aura estimé que des données sont particulièrement sensibles et que la consultation directe de ces dernières par le patient risque de lui porter préjudice, le patient ne pourra exercer son droit de consultation que par l'intermédiaire d'un praticien professionnel qu'il aura choisi...

Il s'agira de tenir compte de ces nuances du droit à la consultation lors de l'informatisation des données, et ce, afin d'éviter que le patient n'ait directement accès à l'une des données concernées ci-dessus, en suite de sa demande de consultation du dossier informatisé.

- Le patient a également le droit d'obtenir, au prix coûtant, une copie du dossier le concernant ou une partie de celui-ci, à moins que le praticien dispose d'indications claires selon lesquelles le patient subit des pressions afin de communiquer son dossier à des tiers (article 9, §3 de la loi sur les droits du patient).

- En pratique, à qui va s'adresser le patient pour exercer son droit de consultation?

Au regard de la loi sur la vie privée, le patient doit s'adresser au responsable du traitement. Toutefois, en application du principe du secret médical, ce dernier ne pourrait statuer que s'il est le médecin en charge de ce patient. À défaut, le responsable du traitement devra répercuter la demande du patient à la personne habilitée à y répondre.

Dans un hôpital, il semble opportun que le patient désigne un « médecin-référent », qui participe aux soins de santé qui lui sont prodigués et qui sera la personne habilitée à répondre à sa requête, en suite de la demande formulée au responsable du traitement.

C'est aussi ce médecin de référence (ex : médecin chef de service) qui pourra décider si le dossier peut être « communiqué » au patient au regard d'éventuelles pressions de tiers.

- Rappelons enfin que le patient devrait avoir le droit de demander, quand il le souhaite, *la liste des personnes qui ont accédé à Ses données* (**contrôle a posteriori** des flux des données au sein du service ou de l'hôpital). Le patient s'adressera alors au responsable du traitement qui répercutera la demande à la personne la plus compétente en la matière (service informatique, conseiller en sécurité, etc.).

f.1.2. Le droit d'opposition au traitement des données

Le patient a le droit de s'opposer à ce que ses données à caractère personnel le concernant fassent l'objet d'un traitement.

Ce droit d'opposition se justifie au nom du droit à l'autodétermination informationnelle de tout individu et est inscrit sous deux formes différentes dans deux sources juridiques.

D'une part, *la loi vie privée, en son article 12, §1, al.2.* prévoit que le patient peut se prévaloir de *raisons sérieuses et légitimes* tenant à une situation particulière pour s'opposer au traitement de ses données (Ceci dit, la tenue d'un dossier médical relevant d'une obligation déontologique et légale, l'on peut se demander dans quelle mesure un patient pourrait s'opposer à la tenue d'un dossier « minimum » le concernant).

D'autre part, la théorie du *secret médical partagé* implique que le patient puisse *s'opposer* à tout moment à ce qu'une donnée – même exacte ou pertinente –, soit *communiquée* d'un professionnel des

soins de santé à l'autre et ce, *même sans raison légitime et sérieuse.* Cela implique que le patient doit être préalablement informé de toute communication entre les professionnels, ou à tout le moins des modalités de fonctionnement du réseau impliquant des transferts « potentiels » de données entre ces professionnels (cf. supra).

Pour le cas où le patient s'opposerait à ce qu'une ou plusieurs données soient communiquées à différents professionnels, la qualité du système informatique risque d'être amenuisée. Comment veiller en ces circonstances au caractère complet et exact des informations mises à disposition des professionnels du service (cf. loi vie privée) ? Le praticien devra faire preuve de conviction à l'égard du patient et l'avertir des risques liés à la non-communication de l'information. Dans le cas du refus du patient, il semble judicieux que le médecin indique que des données sont manquantes (sans préciser lesquelles bien entendu). Ainsi, les autres praticiens seront avertis du caractère incomplet des informations mises à leur disposition. Le responsable du traitement devrait également être averti de cet exercice du droit d'opposition.

Notons qu'au cours de son hospitalisation, le patient pourrait, s'il a des souhaits particuliers quant à la (non) informatisation de certaines données sensibles, demander que ses souhaits soient inscrits et accessibles sur ordinateur par les utilisateurs du réseau.

f.1.3. Le droit de rectification, de suppression et d'interdiction d'utilisation de certaines données

- L'article 12 , §1 al.1 de la loi vie privée dispose que le patient a le droit d'obtenir, sans frais, la rectification de toute donnée à caractère personnel inexacte qui le concerne. Le patient adressera une requête en ce sens au responsable du traitement.

L'application de ce droit aux données à caractère personnel relatives à la santé est délicate. Quand peut-on affirmer l'inexactitude d'une donnée médicale parfois empreinte de subjectivité et d'appréciations hypothétiques ?

Indépendamment de ce problème d'appréciation, l'on peut affirmer que le responsable du traitement ne pourra intervenir directement à propos d'une donnée que s'il est le professionnel des soins de santé qui a en charge le patient ou son médecin référent. Si ce n'est pas le cas, le responsable du traitement répercutera la requête au praticien qui a encodé les données et qui est dès lors habilité à procéder à la rectification.

- L'article 12, §1 al. 5 confère le droit au patient d'obtenir, sans frais, la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel qui le concerne et qui, compte tenu de la finalité du traitement poursuivie, est incomplète ou non pertinente, ou dont l'enregistrement, la communication sont interdits ou encore qui a été conservée au-delà de la période autorisée.

Toutefois, comme on l'a vu, en matière de droit médical, la portée de ce droit est plus large. Le patient a le droit de demander la suppression d'une donnée encodée destinée à être « communiquée » même si la donnée est exacte, complète et pertinente.

Ici encore, le patient s'adressera au responsable du traitement qui répercutera la requête au praticien qui a encodé la donnée litigieuse.

- Que ce soit dans le cadre d'une demande de rectification ou de suppression d'une donnée, le praticien concerné et le patient devraient à tout le moins avoir eu un entretien et pu dialoguer sur la contestation. Pour le cas où le praticien signalerait au responsable du traitement que, selon lui, la donnée ne peut être corrigée ou supprimée, le patient pourra éventuellement s'adresser à la Commission de la protection de la vie privée ou au président du tribunal de première instance de son domicile siégeant en référé (cf. infra).

Une médiation, telle que prévue par la loi relative aux droits du patient, entre le praticien qui a encodé la données et le patient pourrait s'avérer utile.

f.1.4. Le droit de porter plainte

En cas de non-respect de ses droits, le patient peut porter plainte. Différentes possibilités de recours sont offertes au patient, en fonction de la loi et des droits en cause.

- En application de la loi vie privée, le patient peut déposer plainte auprès du responsable du traitement pour non respect des droits qui lui sont conférés par ladite loi. Il peut également adresser une plainte auprès du tribunal de première instance de son domicile siégeant en référé ou adresser une plainte auprès de la Commission de protection de la vie privée, dans la mesure où cette plainte a trait à sa mission de protection de la vie privée. En ce dernier cas, après l'examen de la recevabilité de la demande de la personne concernée, la Commission accomplit d'abord toute mission de médiation qu'elle juge utile.

- Le patient peut également déposer plainte au pénal, dès lors que des violations de dispositions de la loi du 8 décembre 1992 érigées en infractions ont été commises ou que d'autres infractions sont en cause (par exemple la méconnaissance du secret professionnel (art. 458 Code pénal)).

- Le patient peut aussi introduire une action en responsabilité civile s'il a subi un dommage en suite du comportement litigieux en cause.

- En vertu de la loi sur les droits du patient, ce dernier peut saisir la fonction de médiation de l'hôpital compétente pour toute plainte concernant l'exercice des droits qui lui sont reconnus en vertu de ladite loi, en ce compris le droit à la protection de la vie privée.

f.1.5. Le droit à la réparation du préjudice

- En vertu de la loi vie privée, le patient a le droit de demander au responsable du traitement la réparation du dommage causé par un acte contraire aux dispositions déterminées par la loi vie privée (art. 15bis loi vie privée). L'utilisation de données inexactes, ayant entraîné des conséquences dommageables, peut être ainsi visée dans la mesure où la loi vie privée exige l'utilisation de données de qualité (cf. supra IV, e.2.).

Il faut savoir que dans ce cas, le patient ne devra pas rapporter la preuve de la faute du responsable ; c'est à ce dernier à prouver que le fait générateur du dommage ne lui est pas imputable pour être exonéré de toute responsabilité.

- Au-delà, en vertu du droit commun, le patient peut toujours introduire une action en responsabilité civile – ou pénale s'il y a infraction – à l'égard de la personne qu'il estime responsable du dommage qu'il a subi. Il lui revient alors de démontrer la faute du praticien et le lien de causalité entre cette faute et le dommage subi.

f.2. L'obligation de loyauté du patient ?

Il paraît nécessaire que le patient fournisse des informations exactes et pertinentes afin de recevoir des soins de santé de qualité. À défaut d'obligation légale dans le chef du patient, nous ne pouvons que recommander aux praticiens d'user de leur pouvoir de conviction en la matière. Il faut signaler au patient que le défaut ou l'inexactitude de l'information qu'il fournit aura non seulement un effet négatif sur le fonctionnement de la banque de données mais aussi et plus

fondamentalement sur lui, sur l'adéquation des soins qui pourront lui être prodigués.

Par ailleurs, l'on rappellera que le patient est plus à même de confier des informations lorsqu'un climat de confiance optimal s'est instauré entre les protagonistes... Lui faire connaître ses droits l'aidera sans doute.